

# **EXHIBIT 9**

**From:** Brown, Timothy [/O=SOLARWINDS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=2C7BCDFD72B7408CB161AB787299E231-TIMOTHY BROWN]  
**Sent:** 12/14/2017 1:58:14 PM  
**To:** Johnson, Rani [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=61ad383fe3474bf084190056f2ce567b-johnson, rani]  
**Subject:** RE: 2018 Roadmap Overview / Team Goals Review  
**Attachments:** Tim Brown 90 Days.pptx

This was a combination of my 90days. Not really the roadmap goals. Here are the goals that map to Joe's goals.  
 Security Operations Goals

1. Leverage scale & synergies to optimize operations and drive technical differentiation (Joe)
  - a. Create consistent security practices that can be shared across the organization. Share vulnerability and threat intel, Security operations best practices, measurement and monitoring. Create a loosely coupled global security operations function that works across core, msp and cloud.
2. Drive Technology & Systems Excellence (Joe)
  - a. Proactively manage and measure the security risk for the company. Drive the consolidation of tools utilized for secure code development and security operations. Provide global measurement and monitoring of overall security risk. Drive remediation architecture and design to reduce the risk.
3. Provide Technology & Security Strategy and Agility to Innovate (Joe)
  - a. Drive a security by design process in everything we do. This includes development, operations, architecture, sales, support, marketing, etc. Innovate in our ability to design, detect, respond and recover.
4. Develop High Performance Team Culture (Joe)
  - a. Develop security skills, threat intelligence knowledge, security by design and product knowledge. Continue to build the team's skills by self-learning, internal training, conferences, peer sessions and product specific training. Create opportunities for the team to take on new challenges, new projects and grow their overall skill set

I had a call with John P last week and I'm working on documenting some goals for his group as well.

Tim

**From:** Johnson, Rani  
**Sent:** Thursday, December 14, 2017 3:52 AM  
**To:** Kemmerer, Joel <joel.kemmerer@solarwinds.com>; Brown, Timothy <timothy.brown@solarwinds.com>; Mills, David <David.Mills@solarwinds.com>  
**Subject:** 2018 Roadmap Overview / Team Goals Review

Hi Guys,

Can you send me the slides you presented in your Roadmap / Goal reviews.

-----Original Appointment-----

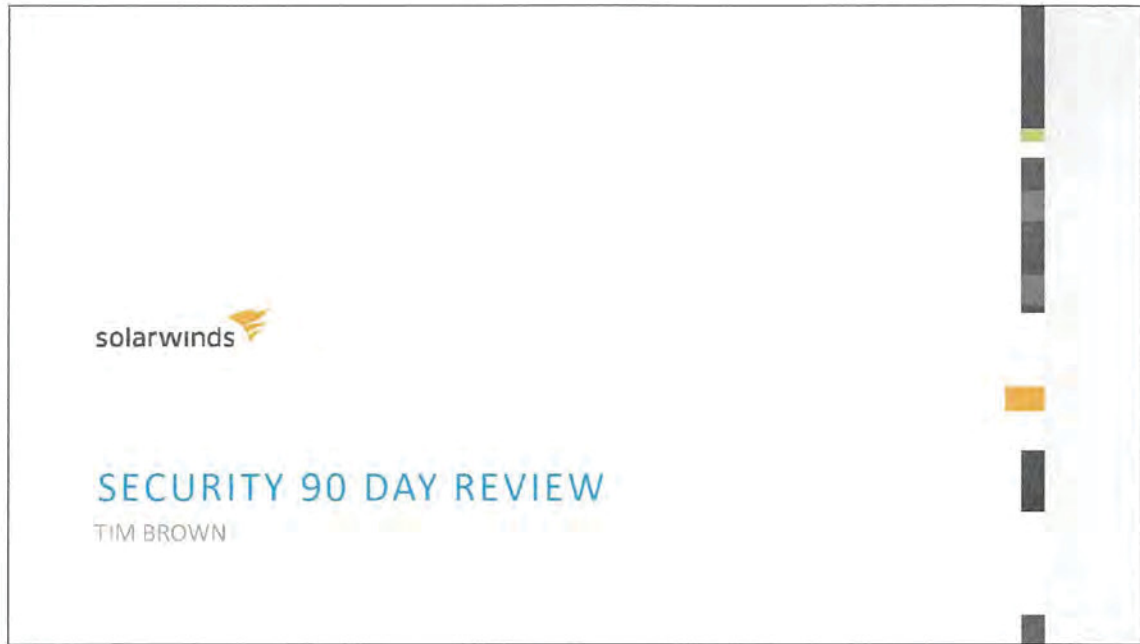
**From:** Johnson, Rani  
**Sent:** Monday, November 20, 2017 10:34 AM  
**To:** Johnson, Rani; Kemmerer, Joel; Brown, Timothy; Mills, David  
**Subject:** Biz Apps 2018 Roadmap Overview / Team Goals Review



**When:** Tuesday, December 5, 2017 4:00 PM-5:00 PM (UTC-06:00) Central Time (US & Canada).

**Where:** Rani's Office

High level overview of 2018 key projects/ operational initiatives, org structure, 2018 R4R Goals

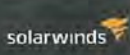


STATE OF SECURITY OPERATIONS DECEMBER 2017	
solarwinds	
Technology	
Network Security Palo Alto	Consistently deployed and managed. But we are currently managing risk from reports and not raw data.
Vulnerability Scanning Manage Rapid 7 and Patching	Good coverage. Managed well and patching consistently. Extending coverage to MSP team. Patching Cloudability.
Anti-Virus Managed SEP	Good coverage and managed well. QDR is driving additional adoption across services.
Endpoint Encryption BitLocker	Some false starts with deployment. Plan in place to continue deployment.
Endpoint DLP Netskope	Deployment plan is on track for deployment in Q4.
Identity Management Okta, Thycotic SS, AD, Linux	AD accounts managed fairly well but needs inspection and monitoring. No consistent identity plan for user or for administrators. Many gaps, inconsistent management.
Security Log Management (SIEV)	LEM is working for the things we are monitoring. Alerting is functioning well. Missing threat intel integration and "threat hunting function".
Incident Response	Running wdr and tested many times. But requires a refresh and training of additional people.
Internal security backlog management and prioritization	Managed and monitored well for core IT systems. Tul/Web Domain are in very good shape. Dev domain is still behind. Linkage between Dev and Tul are of a concern.
Security Training employee	Very little, very limited.
Data Classification	Classification policy is good and good security system in place.
PEN Testing	No internal and external penetration or external security. Need to do a lot of work.
Policies Security, Data Retention, DR	Policies are getting better with GDPR as a driver. Still more to do if we are going to measure ourselves against NIST or complete an ISO Audit. Still missing a number of standard policies.
Operations review Helpdesk, HR, Support	Worked on training, better on security, compliance. Could be more in GDPR. Need to do a lot of work on documentation and training.



**Q&A**



**A proactive security model**


**Risk Mitigation Plan for IT Security Operations**

Lock down our critical assets that could cause a major event

- External PEN test of our environment - Provides a baseline
- Lock down administrative access and improve identity management processes and procedures
- Implement Web Application Firewall to protect our critical apps and content

Improve Cyber Hygiene so we are not a target of opportunity

- Improve coverage for endpoint security, incident response, threat management
- Improve system security coverage, monitoring and patching
- Implement DLP on line endpoints
- Implement security training for all employees

Focus on security areas that provide the biggest impact

- Coordinate IT Security Ops activities across all organizations - Standardize policies, create best practices and coordinate the risk management effort for the organization
- Create sign approved security questionnaire answers
- Reduce the number of security incidents by implementing industry standard best practices

Overall Budget Request: Assumes cross company adoption of all security controls

Security Program Manager	\$180 IT/Dev Ops	
Security Architect	\$180 IT/Dev Ops	
Application Firewall	\$40K per year	
Internal/External PEN test	\$100K	
Company wide Security Training	\$30K	
Secure development training	\$30K	
Commercial application code scanner	\$70K	
<b>Total</b>		<b>\$680K + 30%</b>

Time of 4 Security Champions

**Risk Mitigation Plan for Product Security/Dev Ops**

Establish a global, cross-pillar Security Champions – Product team members with 30% of their time dedicated to security. Dotted line report to VP Security Architecture

- Internal Training and Outreach
- Coordinate internal product security testing and application vulnerability scanning
- Internal bug bounty program
- Product Management and Engineering management coordination
- Measurement of risk and effectiveness of program per product line
- Invest in Commercial code scanning tool
- Invest in developer security training

**Risk of Non-Investment**

- Current state of security leaves us in a very vulnerable state for our critical assets. A compromise of these assets would damage our reputation and financially.
- Lack of cyber hygiene leaves us open to being a target of opportunity and a compromise will create downtime and lost revenue
- We have had 22 reported security incidents this year. Reactive responses costs significantly more than being proactive.
- We have lost a renewal of DPA for Accenture (192K) due to utilizing free code scanning tools that did not find all vulnerabilities.
- Without training our employees will continue to be one of our biggest risks
- Appropriate security policies, procedures, training, PEN testing are required by our commercial customers and asked for in qualifying questionnaires. Without appropriate answers we will lose business